UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

JOHN DOE, Individually, and on behalf of all others similarly situated,

Plaintiff

v.

VILLAGE PRACTICE MANAGEMENT COMPANY, LLC D/B/A VILLAGE MEDICAL D/B/A VILLAGEMD

Defendant.

Civil Action No. 24-cv-2882

CLASS ACTION COMPLAINT

Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated (hereinafter "Plaintiff") brings this Class Action Complaint against Defendant, VILLAGE PRACTICE MANAGEMENT COMPANY, LLC d/b/a VILLAGE MEDICAL d/b/a VILLAGEMD ("Village" or "Defendant"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

INTRODUCTION

1. Plaintiff brings this class action to address Defendant's outrageous, illegal, and widespread practice of disclosing the confidential Personally Identifying Information[1] ("PII") and/or Protected Health Information[2] ("PHI") (collectively referred to as "Private Information")

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as

of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"), Google, LLC ("Google"), and others ("the Disclosure").

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as Defendant,' that "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[3] OCR and FTC agree that such tracking technologies, like those present on Defendant's website, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[4] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation,

---

individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Village is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services (July 20, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last accessed March 21, 2024), **attached as Exhibit A.**

[4] *Id.*

health, or physical safety of the individual or to others."[5]

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider may disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. On March 18, 2024, HHS updated its December 2022 bulletin,[6] reiterating:

> **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[7,8]

---

[5] *Id*.
[6] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. Apr. 3, 2024).
[7] Citing *to* 45 CFR 164.508(a)(3); s*ee also* 45 CFR 164.501 (definition of "Marketing").
[8] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Updated March 18, 2024),

6. Headquartered in Chicago, Illinois, Defendant is a massive medical system which provides treatment to patients in Illinois and across the United States, including in Colorado, Texas, Indiana, Kentucky, Michigan, Arizona, Georgia, Nevada, Florida, New Jersey, Rhode Island, Massachusetts, and New Hampshire.[9]

7. Despite its unique position as a massive and trusted healthcare provider, Defendant knowingly configured and implemented into its website, https://www.villagemedical.com/ (the "Website") code-based tracking devices known as "trackers" or "tracking technologies," which collected and transmitted patients' Private Information to Facebook, and other third parties, without patients' knowledge or authorization.

8. Defendant encourages patients to use its Website, along with its various web-based tools and services (collectively, the "Online Platforms"), to learn about Village on its main website page,[10] to research treatment services,[11] to find providers,[12] to schedule appointments,[13] to access a patient portal[14] and more, including to find locations,[15] to research insurance information,[16] and to learn about health information via a blog.[17]

9. When Plaintiff and Class Members used Defendant's Websites and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendant embedded pixels from Facebook and others into its

---

avail at. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis in original) (last acc. Apr. 3, 2024).
[9] https://www.villagemedical.com/locator (last accessed Apr. 3, 2024).
[10] https://www.villagemedical.com/ (last accessed Apr. 3, 2024).
[11] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).
[12] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).
[13] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. Apr. 3, 2024).
[14] https://www.villagemedical.com/patient-portal (last acc. Apr. 3, 2024).
[15] https://www.villagemedical.com/locator (last acc. Apr. 3, 2024).
[16] https://www.villagemedical.com/insurance (last acc. Apr. 3, 2024).
[17] https://www.villagemedical.com/journey-to-well (last acc. Apr. 3, 2024).

Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

10. A tracker (also referred to as "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[18] When a person visits a website with an tracker, it tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[19] Then, the tracker transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[20]

11. Among the trackers Defendant embedded into its Website is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a website user's device and the URLs and domains they visit.[21] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[22] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[23]

---

[18] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[19] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[20] *Id.*
[21] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[22] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[23] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to

12. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiff's and Class Members' private health information, alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

13. Facebook encourages and recommends use of its Conversions Application Programming Interface ("CAPI") alongside use of the Meta Pixel.[24]

14. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interactions from the website owner's private servers, which transmits the data directly to Facebook, without involvement from the website user's browser.[25, 26]

15. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad

---

personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

[24] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[25] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[26] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

blockers or other denials of consent by the website user that would prevent the Meta Pixel from sending website users' Private Information to Facebook directly. For this reason, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[27]

16. Defendant utilized data from these trackers to market their services and bolster their profits. Facebook utilizes data from the Meta Pixel and CAPI to build data profiles for the purpose of creating targeted online advertisements and enhanced marketing services, which it sells for profit.

17. On information and belief, the information that Defendant's Meta Pixel, and possibly CAPI, sent to Facebook included the Private Information that Plaintiff and the Class Members submitted to Defendant's Websites and Online Platforms, including, *inter alia,* the pages they viewed and the buttons they clicked; their statuses as patients; the treatment services they viewed;[28] the medical providers they viewed;[29] appointments they scheduled;[30] activities on the patient portal;[31] as well identifying information, such as IP addresses.

18. Such information allows third parties (e.g., Facebook) to learn of a particular individual's health conditions and seeking of medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers, who then target Plaintiff and Class Members with online advertisements, based on the information they communicated to Defendant

[27] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).

[28] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).
[29] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).
[30] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. Apr. 3, 2024).
[31] https://www.villagemedical.com/patient-portal (last acc. Apr. 3, 2024).

via the Website. Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

19. In addition to the Facebook Pixel, and likely CAPI, on information and belief, Defendant installed other tracking technologies, which operate similarly to the Meta Pixel and transmitted Plaintiff's and Class Members' Private Information to unauthorized third parties.

20. Healthcare patients simply do not anticipate that their trusted healthcare provider will send their private health information to a hidden third party—let alone Facebook, a company with a sordid history of violating consumer privacy in pursuit of ever-increasing advertising revenue.

21. Neither Plaintiff nor any Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or other third parties uninvolved in their treatment.

22. Despite willfully and intentionally incorporating the Meta Pixel, potentially CAPI, and other third-party trackers into its Website and servers, Defendant have never disclosed to Plaintiff or Class Members that it shared their Information with Facebook, and possibly others.

23. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

24. Defendant owed common law, statutory, and regulatory duties to keep Plaintiff's and Class Members' communications and Private Information safe, secure, and confidential.

25. Upon information and belief, Village utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new

patients, and generate sales.

26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard their information from unauthorized disclosure.

27. Defendant breached its common law and statutory obligations to Plaintiff and Class Members by, *inter alia*, (i) failing to adequately review their marketing programs and web-based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook, and others; (v) failing to protect Private Information and take steps to block the transmission of Plaintiff's and Class Members' Private Information through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor their Website to maintain the confidentiality and integrity of patient Private Information.

28. Plaintiff seeks to remedy these harms and bring causes of action for: (I) Negligence; (II) Invasion of Privacy—Intrusion Upon Seclusion; (III) Breach of Implied Contract, (IV) Unjust Enrichment; (V) Breach of Fiduciary Duty, and (VI) Violation of the Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.

PARTIES

29. Plaintiff, JOHN DOE, is a natural person and a resident and citizen of Massachusetts, where he intends to remain, with a principal residence in Quincy, Massachusetts in Norfolk County. Plaintiff has been a patient of Village since January 2023, and is a victim of

Defendant's unauthorized Disclosure of Private Information.

30. Defendant VILLAGE PRACTICE MANAGEMENT COMPANY, LLC d/b/a VILLAGE MEDICAL d/b/a VILLAGEMD ("Village" or "Defendant"), is a limited liability company organized and existing under the laws of the State of Delaware, with a principal place of business located at 433 W. Van Buren Street, Suite 510 S. Chicago, Illinois 60607 in Cook County.[32]

31. Defendant's Registered Agent for Service of Process is Illinois Corporation Service Company, 801 Adlai Stevenson Drive, Springfield, Illinois 62703-4261.

JURISDICTION AND VENUE

32. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this State; it maintains its principal place of business and headquarters in Illinois; and committed tortious acts in this State.

33. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendant.

34. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

35. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the

[32] *See* Secretary of the Commonwealth of Massachusetts, Business Entity Summary, "Village Practice Management, LLC" available at https://corp.sec.state.ma.us/CorpWeb/CorpSearch/CorpSummary.aspx?sysvalue=NrygV5fu.tPxNet6g3I21S_x5V.4vBXR40_T3cD5p.E- (last acc. Mar. 28, 2024).

events and omissions giving rise to Plaintiff's claims occurred in this district.

COMMON FACTUAL ALLEGATIONS

A. Background

36. Defendant is an Illinois healthcare provider which renders primary care medical treatment to patients across the country under a mission "[t]o make primary care more caring."[33]

37. Village represents to patients and prospective patients that:

> **How we make you primary.**
>
> We take a "coordinated care" approach to your health. That means you receive the time and attention you need from an entire care team who coordinates with your primary care provider. This way, we can help you with annual check-ups, lab work, illness + injury treatment, even specialist referrals and medication management. And we welcome most insurance and Medicare Advantage plans.[34]

38. Defendant provides treatment services to patients in Illinois, as well as in Colorado, Texas, Indiana, Kentucky, Michigan, Arizona, Georgia, Nevada, Florida, New Jersey, Rhode Island, Massachusetts, and New Hampshire.[35]

39. In fact, as Village describes, "[o]ur teams live and work near our patients, in over 680 practices across cities, suburbs, and rural areas, including inside many Walgreens locations. This way we're never too far from your home. Or ours."[36]

40. Defendant's primary care medical services include: "Anywhere visits and same-day appointments" ("Get the care you need, when you need it. You can see a primary care provider at one of our practices, through a virtual visit on your phone or computer, or in-person at home for patients who need it."); Chronic care management ("We can help you manage a wide range of

[33] https://www.villagemedical.com/ (last acc. Apr. 3, 2024).
[34] *Id*.
[35] https://www.villagemedical.com/locator (last acc. Apr. 3, 2024).
[36] https://www.villagemedical.com/ (last acc. Apr. 3, 2024).

diseases including diabetes, hypertension, COPD (chronic obstructive pulmonary disease), congestive heart failure and endocrine disorders…"); " Coordination for your specialty care[;]" treatment for "Illness and injuries" ("We can help you take care of coughs, colds, the flu, ear infections and more. Before you head to urgent care, reach out for a phone consultation or same-day appointment."); as well as home care, Village Medical at Home; on-site laboratories; Annual Well Visits; and patient portal services, "24/7 account access" ("Schedule appointments, get reminders, view test and imaging results and more on your smartphone via the Village Medical Mobile App or on the web via your patient portal.").[37]

41. In fact, Village specifically promotes "Same-day appointments[;] Clinic, in-home & virtual visits[;]" and its convenient blood and other laboratory diagnostic testing:[38]

42. According to Defendant, "Village Practice Management Company, LLC ('VillageMD' or 'We') is comprised of various entities that provide healthcare and related services to individuals throughout the United States of America. The following entities make up the VillageMD family: • Village Medical Primary Care Clinics* • Village Medical at Walgreens • Village Medical at Home • Village Medical Pharmacy [and] Village Medical Physical Therapy."[39]

43. On information and belief, Village "delivers services to around 1.6 million patients,

[37] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).
[38] https://www.villagemedical.com/ (last acc. Apr. 3, 2024).
[39] Village Medical, *Terms of Use*, Effective Date Oct. 15, 2019, Rev. Aug. 14, 2020, avail. at https://www.villagemedical.com/terms-and-conditions **attached as Exhibit B.**

[…and] [i]ts 2021 revenue was about $1.3 billion…"[40]

44. Defendant serves many of its patients via its Websites and Online Platforms, which Village encourages patients to use to learn about Village on its main website page,[41] to find treatment services,[42] to find providers,[43] to schedule appointments,[44] to access a patient portal[45] and more, including to find locations,[46] to research insurance information,[47] and to learn about health information via a blog.[48]

45. In furtherance of that goal, Defendant purposely installed the Meta Pixel and other trackers onto its Website, for the purpose of gathering information about Plaintiff and Class Members to further its marketing efforts. But Defendant did not only generate information for its own use: it also shared patient information, including Private Information belonging to Plaintiff and Class Members, with Facebook, other unauthorized third parties.

46. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

47. Facebook operates the world's largest social media company and generated $117

[40] Robert Holly, Home Health Care News, *VillageMD to Drive 'Tremendous Long-Term Growth' for Walgreens Health,* Jan. 14, 2022, avail. at https://homehealthcarenews.com/2022/01/villagemd-to-drive-tremendous-long-term-growth-for-walgreens-health/#:~:text=VillageMD%20delivers%20services%20to%20around,according%20to%20the%20investor%20deck. (last acc. Apr. 3, 2024).
[41] https://www.villagemedical.com/ (last accessed Apr. 3, 2024).
[42] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).
[43] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).
[44] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. Apr. 3, 2024).
[45] https://www.villagemedical.com/patient-portal (last acc. Apr. 3, 2024).
[46] https://www.villagemedical.com/locator (last acc. Apr. 3, 2024).
[47] https://www.villagemedical.com/insurance (last acc. Apr. 3, 2024).
[48] https://www.villagemedical.com/journey-to-well (last acc. Apr. 3, 2024).

billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[49]

48. In conjunction with its advertising business, Facebook encourages and promotes its "Business Tools" to be used to gather customer data, identify customers and potential customers, target advertisements to those individuals, and market products and services.

49. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

50. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, clicks a button, fills out a form, and more.[50] Businesses that want to target customers and advertise their services can also create their own tracking parameters by building a "custom event."[51]

51. The Meta Pixel is a Business Tool used to "track[] the people and type of actions they take" on a website.[52] When an individual accesses a webpage containing the Meta Pixel, the communications with that webpage are instantaneously and surreptitiously duplicated and sent to Facebook, traveling directly from the user's browser to Facebook's server, based off instructions from the Meta Pixel.

---

[49] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

[50] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[51] About Standard and Custom Website Events, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.

[52] Retargeting, META, https://www.facebook.com/business/goals/retargeting.

52. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy, such as a homepage, and disable it on pages that do implicate patient privacy, such as Defendant's "Provider" pages.[53]

53. The Meta Pixel's primary purpose is to enhance online marketing, improve online ad targeting, and generate sales.[54].

54. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[55]

55. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** [Emphasis added.]
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.
> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[56]

56. Facebook boasts to its prospective users that the Meta Pixel can be used to:

---

[53] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).
[54] *See* Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).
[55] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).
[56] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Mar. 19, 2023).

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.

- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.

- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[57]

57. Facebook likewise benefits from Meta Pixel data and uses it to enhance its own ad targeting abilities.

ii. Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Meta Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Meta Pixel

58. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

59. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

60. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP

[57] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Mar. 19, 2023).

Responses, along with corresponding cookies.[58]

61. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

62. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information. The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

63. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

64. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

65. In this way, the Meta Pixel acts much like a traditional wiretap: intercepting and transmitting communications intended only for the website host and diverting them to Facebook.

66. Separate from the Meta Pixel, third parties place cookies in the browsers of web users. These cookies can uniquely identify the user, allowing the third party to track the user as they browse the internet—on the third-party site and beyond. Facebook uses its own cookie to

[58] "Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

identify users of a Meta-Pixel-enabled website and connect their activities on that site to their individual identity. As a result, when a Facebook account holder uses a website with the Meta Pixel, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the user associated with the information it has intercepted.

67. With substantial work and technical know-how, internet users can sometimes circumvent these browser-based wiretap technologies. To counteract this, third parties bent on gathering data implement workarounds that are difficult for web users to detect or evade. Facebook's workaround is Conversions API, which "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[59] This makes Conversions API a particularly effective tool because it allows sends Facebook data directly from the website server to Facebook, without relying on the user's web browser. Notably, client devices do not have access to host servers containing Conversions API, and thus, they cannot prevent (or even detect) this transmission of information to Facebook.

68. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the website server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[60] Consequently, if a website owner utilizes the Meta Pixel on its website, it is also reasonable to infer that it implemented the Conversions API

[59] About Conversions API, META, https://www.facebook.com/business/help/2041148702652965 (last visited May 15, 2023).
[60] *See* Best Practices for Conversions API, META, https://www.facebook.com/business/help/308855623839366 (last visited May 15, 2023).

on its website server(s), in accordance with Facebook's documentation.

69. The Meta Pixel, Conversions API, and other third-party trackers do not provide any substantive content on the host website. Rather, their only purpose is to collect information to be used for marketing and sales purposes.

70. Accordingly, without any knowledge, authorization, or action by a user, a website owner can use its website source code to commandeer its users' computing devices and web browsers, causing them to invisibly re-direct the users' communications to Facebook, and others.

71. In this case, Defendant employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

72. Consequently, when Plaintiff and Class Members visited Defendant's Websites and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

73. On information and belief, Defendant also employed other trackers which likewise transmitted Plaintiff's and the Class Members' Private Information to third parties without Plaintiff's and Class Members' knowledge or authorization.

iii. Defendant Violated Its Own Privacy Policies

74. Defendant maintains and is covered under a Joint Notice of Privacy Practices,[61] ("Notice of Privacy Practices") and a website Terms of Use[62] (collectively, "Privacy Policies") which are posted on its Website.

---

[61] Village, *Joint Notice of Privacy Practices*, avail. at https://www.villagemedical.com/hubfs/Documents/Compliance/VMD%20NPP%20-%201-30-2024.pdf (last acc. Apr. 3, 2024), **attached as Exhibit C.**

[62] Village Medical, *Terms of Use*, Effective Date Oct. 15, 2019, Rev. Aug. 14, 2020, avail. at https://www.villagemedical.com/terms-and-conditions (last acc. Apr. 3, 2024), **Exhibit B.**

75. Defendant's Notice of Privacy Practices "applies to the following organizations (collectively, "Village Medical"): • Village Medical and its medical staff • Village Medical Physical Therapy and Rehabilitation and its medical staff • Village Medical at Home and its medical staff • Village Medical Pharmacy and its medical staff."[63]

76. In the Notice of Privacy Practices, Village represents, acknowledges, and promises patients that:

> Law requires us to keep your identifiable health information private, to provide you with this Notice of our legal duties and privacy practices with respect to your health information and to follow the terms of the Notice as long as it is in effect. If we revise this Notice, we will follow the terms of the revised Notice, as long as it is in effect.[64]

77. Therein, Defendant enumerates certain purposes for which it may disclose health information/Private Information, *inter alia*: for treatment ("We may use or disclose your health information to a physician or other healthcare provider in order to provide care and treatment to you…"); payment; for healthcare operations ("We may use or disclose health information about you to support the programs and activities of Village Medical, such as quality and service improvement, healthcare delivery review, staff performance evaluation, competence or qualification review of healthcare professionals, education and training of physicians and other healthcare providers, business planning and development, business management and general administrative activities…); in a health information exchange; to family and friends; for public health and safety purposes as described; to business associates ("There are some services provided at Village Medical through contracts with business associates. When these services are contracted, we will disclose your health information to the business associate so they can perform the job we

[63] *Joint Notice of Privacy Practices*, **Exhibit C.**

[64] *Id*.

have asked them to do. However, business associates, such as Village Medical, are required by federal law to appropriately safeguard your information."); and for research purposes.[65]

78. None of the purposes for which Village may disclose PHI/health information without written authorization under the Notice of Privacy Practices include the Disclosure of Private Information via the Meta Pixel and other trackers to third parties for marketing purposes.

79. Further, in the Notice of Privacy Practices, Defendant specifically represents, acknowledges, and promises that, "[w]e will not use or disclose your health information, except as described in this document, unless you authorize us, in writing, to do so. […] Specific examples of uses or disclosures requiring written authorization include the use of psychotherapy notes, marketing activities, the sale of your health information and most uses and disclosures for which we are compensated."[66]

80. Moreover, therein, Village states that, "[i]n certain instances, you have the right to be notified in the event that we, or one of our business associates, discover an inappropriate use or disclosure of your health information. Notification of any such use or disclosure will be made in accordance with state and federal requirements."[67]

81. In addition, Defendant maintains a Website Terms of Use, in which Village states:

> Welcome! You have arrived at a website or application (collectively, a "Digital Service") location which is owned and operated by Village Practice Management Company, LLC ("VillageMD" or "We"). […]
>
> This Terms of Use governs your access to and use of the Digital Service, including any content, functionality and services offered on or through the Digital Service. **Please read these Terms of Use carefully before accessing or using the Digital Service, so that you fully understand your rights and responsibilities**.[68]

[65] *Id*.
[66] *Id*.
[67] *Id*.
[68] Village Medical, *Terms of Use*, Effective Date Oct. 15, 2019, Rev. Aug. 14, 2020, avail. at https://www.villagemedical.com/terms-and-conditions (last acc. Apr. 3, 2024), **Exhibit B** (bold emphasis added)

82. In fact, in the Terms of Use, Village specifically represents and promises that "[t]he use of the Digital Service is also governed by the terms of the VillageMD Privacy Policy which are incorporated into these Terms of Use by this reference. Any protected health information collected on the Digital Service will be used and disclosed only in accordance with VillageMD's Notice of Privacy Practices. By using the Digital Service, you consent to all actions taken by us with respect to your information in compliance with the Privacy Policy." [69]

83. In the Terms of Use, Defendant states that it "has business relationships and affiliations with third-party vendors that deliver certain services and content" which include Google Analytics ("We use Google Analytics for tracking queries submitted to ***their*** search engines. We also use Google's DoubleClick technology for tracking our advertisements, enabling "tell-a-friend" social media functionality and providing us with the contact information of users who submit a request for additional information about our services via click-through advertisements…" and Cision, but does not mention Facebook.[70]

84. Nowhere in the Terms of Use does Village disclose its use of the Meta Pixel, or that it will share patients' Private Information, including PHI, with third parties uninvolved in their treatment, for marketing purposes, without their authorization.

85. Despite these representations in its Privacy Policies, Defendant does indeed transfer Private Information to third parties for marketing purposes, without written authorization. Using the Meta Pixel and other tracking technologies, Defendant used and disclosed Plaintiff's and Class Member's Private Information and confidential communications to Facebook, and likely other unauthorized third parties, without written authorization, in violation of Village's Privacy Policies.

---

[69] *Id*.
[70] *Id*. (bold italicized emphasis added).

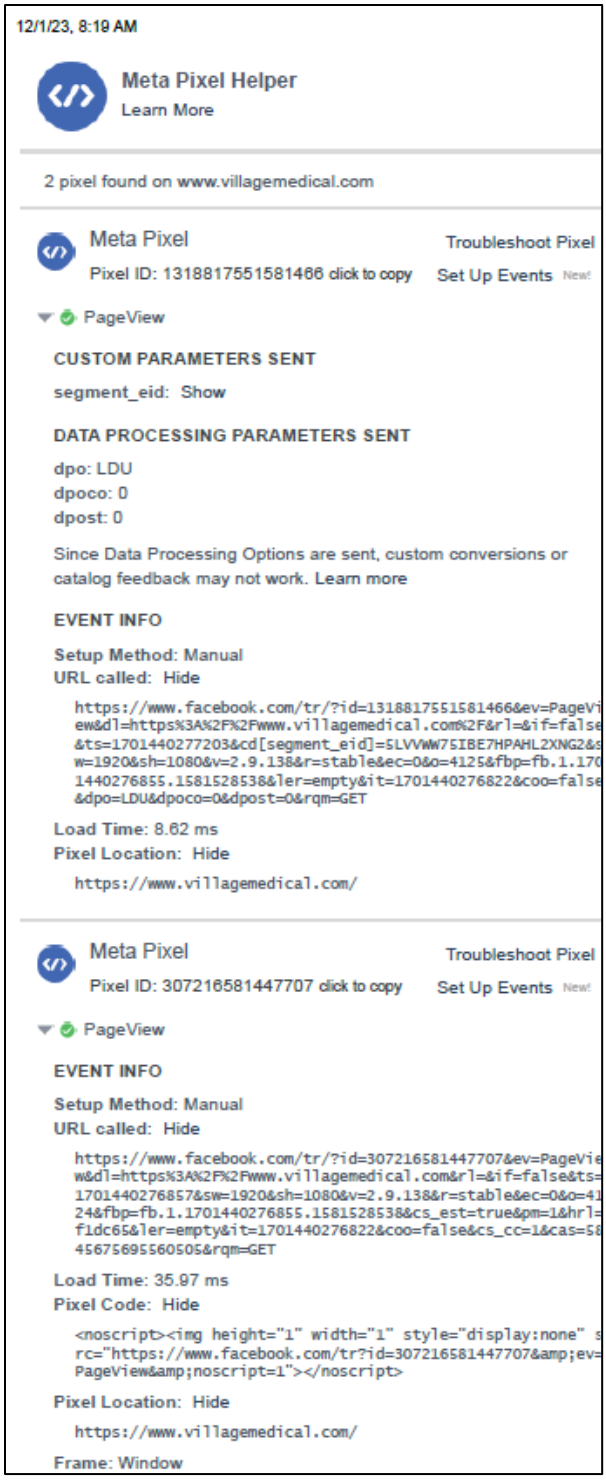
iv. Village Unauthorizedly Disclosed Plaintiff's and the Class's Private Information

86. Defendant disclosed Plaintiff's and Class Members' Private Information and confidential communications to Facebook and other third parties via the Meta Pixel and other tracking technologies for marketing purposes.

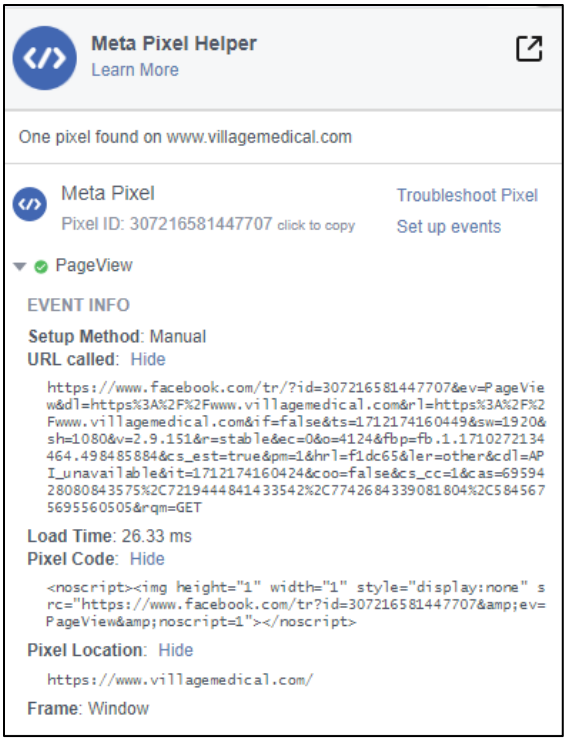
87. On information and belief, through the use of the Meta Pixel, Defendant disclosed to Facebook the Private Information and communications that Plaintiff and the Class Members submitted to Defendant's Website including, *inter alia,* the pages they viewed and the buttons they clicked; their statuses as patients; the treatment services they viewed;[71] the medical providers they viewed;[72] appointments they scheduled;[73] their activities on the patient portal;[74] as well as identifying information, such as IP addresses, and users' "c_user" cookies, which Facebook uses to identify users, and which are transmitted via Meta Pixel "events."

88. For example, as of December 2023, Defendant utilized the Meta Pixel on its main Website page, [75] as shown by the Meta Pixel Helper below:

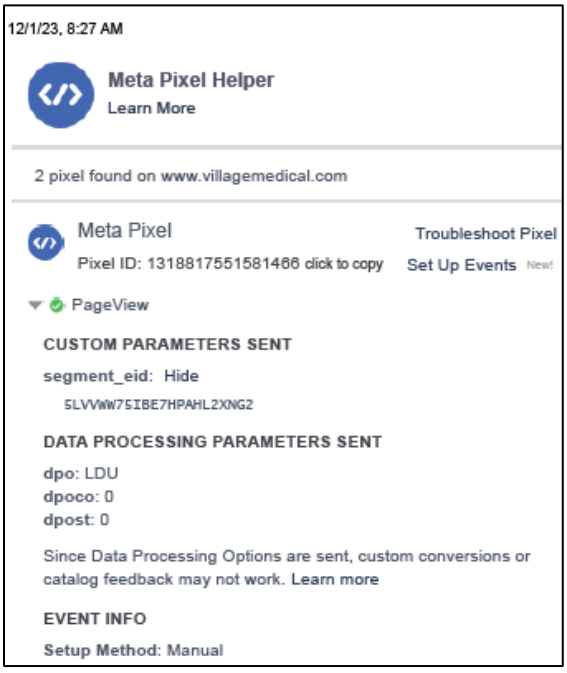
[71] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).
[72] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).
[73] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. Apr. 3, 2024).
[74] https://www.villagemedical.com/patient-portal (last acc. Apr. 3, 2024).
[75] https://www.villagemedical.com/ (last acc. Apr. 3, 2024).



89. In fact, the Meta Pixel remains on the Website homepage as of April 3, 2024:

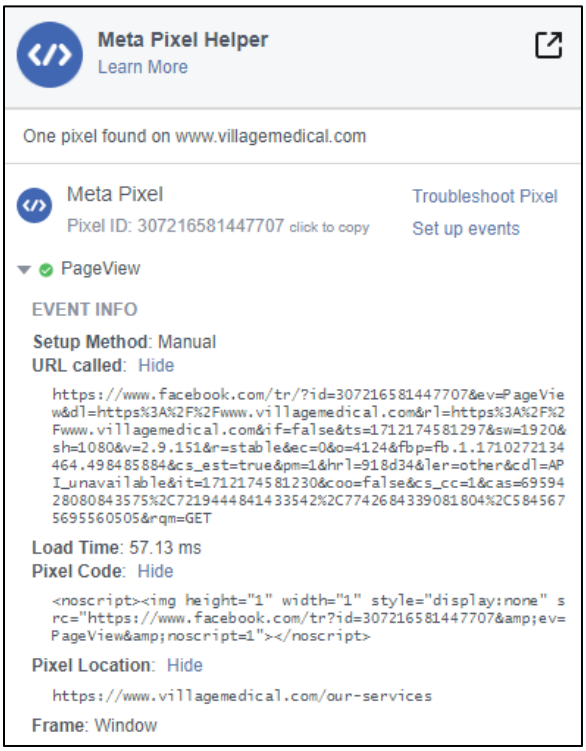


90. Likewise, Defendant utilized at least two (2) Meta Pixels on its "Services" page:[76]

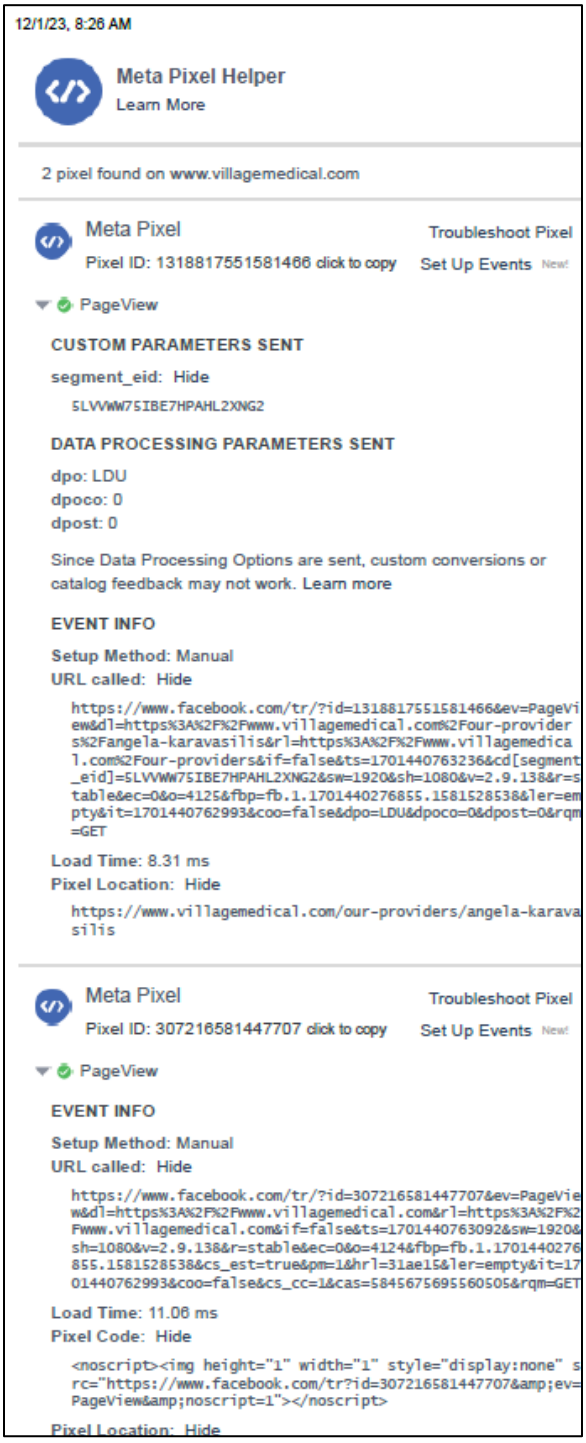


[76] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).

91. Village continues to utilize the Meta Pixel on its Services pages as of April 3, 2024:

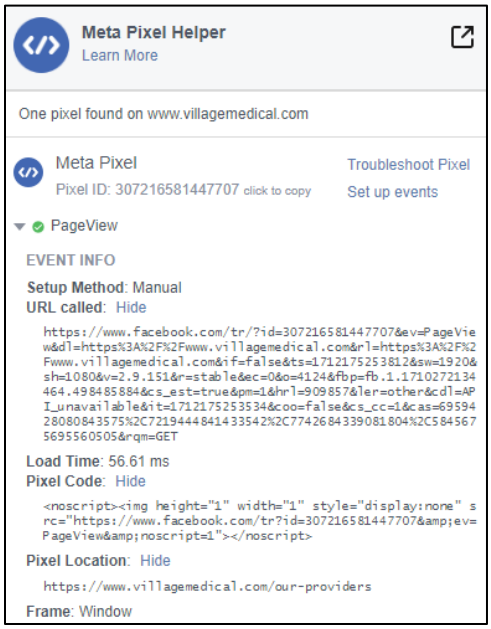


92. Village additionally utilized Meta Pixels on its "Providers" page which patients and prospective patients use to find doctors:[77]

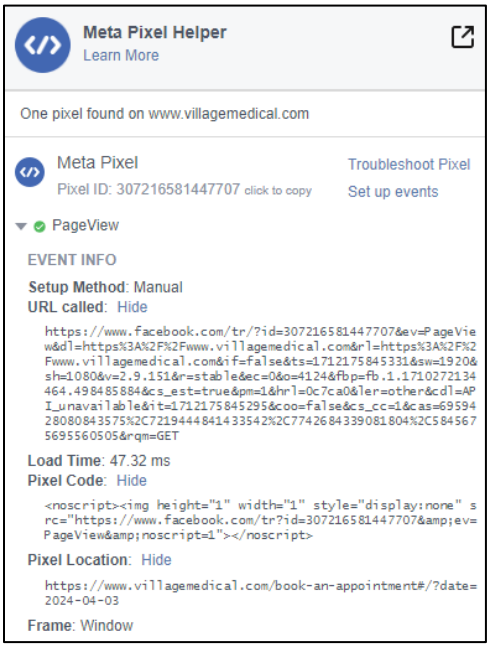


[77] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).

93. Defendant continues to utilize the Pixel on its "Provider" pages as of April 3, 2024:

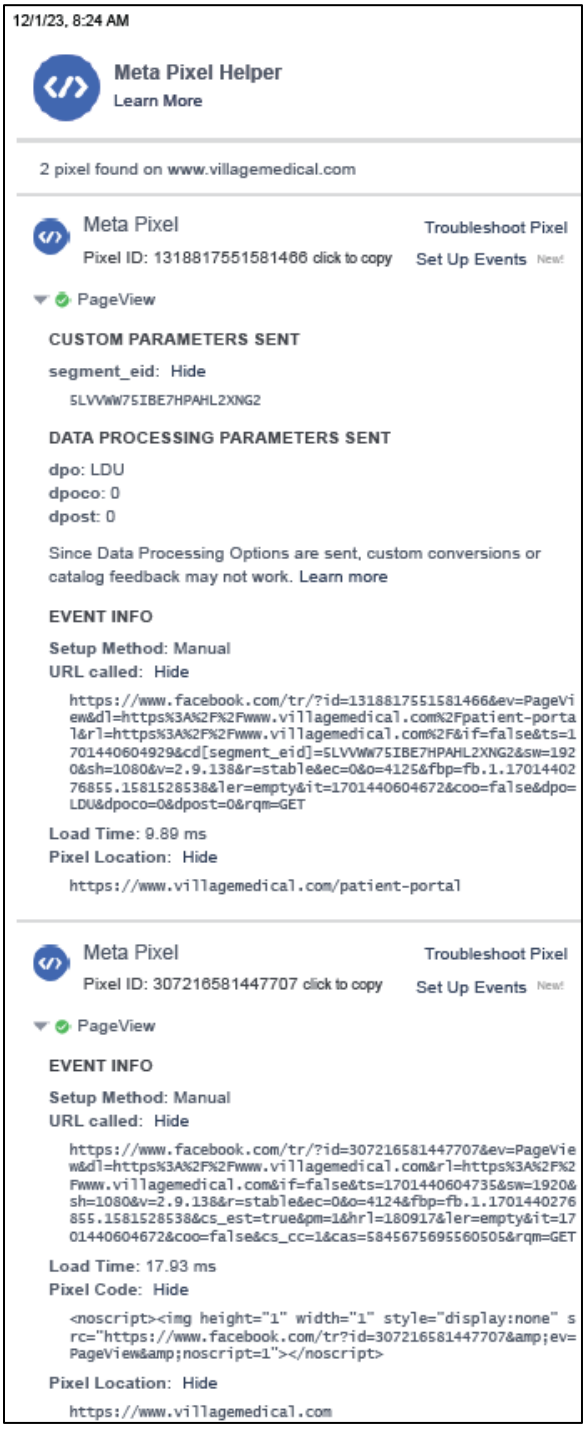


94. Further, Defendant installed the Meta Pixel on pages patients use to make appointments, [78] which remains installed as of April 3, 2024, as shown by the Meta Pixel Helper:



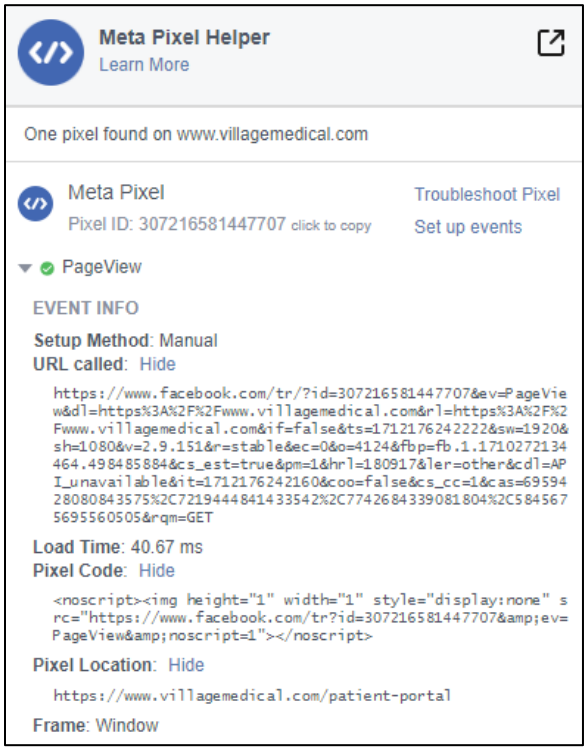
[78] https://www.villagemedical.com/book-an-appointment#/?date=2024-04-03 (last acc. Apr. 3, 2024).

95. Moreover, Village installed and utilizes the Meta Pixel on the pre-portal login page for the patient portal:[79]



[79] https://www.villagemedical.com/patient-portal (last acc. Apr. 3, 2024).

96. As with the other Meta Pixels, Village continues to utilize the Pixel on the pre-portal login, as shown by the Meta Pixel Helper as of April 3, 2024:



97. Accordingly, on information and belief, Defendant has installed and utilizes the Meta Pixel on its patient portal.

98. Lastly, in addition to this information, the Meta Pixel collects and transmits to Facebook other identifying information, including IP addresses, and users' "c_user" cookies, which Facebook uses to identify users, and which are transmitted in Facebook events.

99. Therefore, the Meta Pixel events Village sent to Facebook likely allowed Facebook to connect users,' Plaintiff's and the Class Members,' identities with the details reported within the events.

100. On information and belief, through the use of the Meta Pixel installed on its Online Platforms as described herein, Defendant disclosed to Facebook the Private Information and

communications that Plaintiff and the Class Members submitted to Defendant's Website including, *inter alia,* the pages they viewed and the buttons they clicked; their statuses as patients; the treatment services they viewed; the medical providers they viewed; appointments they scheduled; their activities on the patient portal; as well as identifying information, such as IP addresses, and users' "c_user" cookies.

101. After receiving information from Defendant, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond to your ad."[80] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[81] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[82] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[83]

102. Google and other companies process data in a similar manner and use it to build marketing and other data profiles allowing for targeted online advertising.

103. Defendant could have chosen not to use the Meta Pixel, or it could have configured it to limit the information that it communicated to Facebook, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the

[80] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[81] *Id.*
[82] *Id.*
[83] How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).

Disclosure of Plaintiff and Class Members' Private Information.

104. Along those same lines, Defendant could have chosen not to use other tracking technologies to track Plaintiff and Class Members private communications and transmit that information to unauthorized third parties. It did so anyway, intentionally taking advantage of these trackers despite the harm to Plaintiff and Class Members' privacy.

105. Defendant used and disclosed Plaintiff's and Class Members' Private Information to Facebook, and other third parties for the purpose of marketing its services and increasing its profits.

106. On information and belief, Defendant shared, traded, or sold Plaintiff's and Class Members' Private Information with Facebook, and others in exchange for improved targeting and marketing services.

107. Plaintiff and the Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to third parties uninvolved in their medical care for marketing purposes. Plaintiff and the Class Members were never provided with any written notice that Defendant regularly disclosed its patients' PHI/Private Information to Facebook, and others, nor were they provided any means of opting out of such disclosures, nor did Plaintiff nor the Class Members ever execute a written authorization permitting the Disclosure. Defendant, nonetheless, knowingly disclosed Plaintiff's Private Information, including PHI, to unauthorized entities including Facebook and used that information for its own gain.

108. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

109. Furthermore, Defendant actively misrepresented that it would preserve the security

and privacy of Plaintiff's and Class Members' Private Information, while, in actuality, it was knowingly disclosing this information to unauthorized third parties.

110. By law, Plaintiff and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. Defendant deprived Plaintiff and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff and Class Members' confidential communications, Private Information (Personally Identifiable Information, and Protected Health Information); (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook, and others; (3) profited from the Disclosure; and (4) undertook this pattern of conduct without notifying Plaintiff and Class Members and without obtaining their express written consent.

B. Plaintiff's Experience

111. Plaintiff has been a patient of Defendant since January 2023, approximately, receiving healthcare services from Village and physicians in Village's network, including for mental health treatment at Defendant's clinic in Quincy, Massachusetts.

112. Plaintiff relied on Village's Website and Online Platforms to communicate confidential patient information, beginning in January 2023, and last in October 2023. Specifically, he used the Online Platforms to: find a doctor on the "Find a provider" function;[84] to research primary care and mental health treatment services;[85] and for the patient portal, which he also used to schedule appointments.[86]

113. Plaintiff accessed Defendant's Website and Online Platforms at Defendant's

[84] https://www.villagemedical.com/our-providers (last acc. Apr. 3, 2024).
[85] https://www.villagemedical.com/our-services (last acc. Apr. 3, 2024).
[86] https://www.villagemedical.com/patient-portal (last acc. Apr. 3, 2024).

direction and encouragement. Plaintiff reasonably expected that his communications with Village were confidential, solely between himself and Village, and that, as such, those communications would not be transmitted to or intercepted by a third party.

114. Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to Village's Privacy Policies and the law.

115. On information and belief, through its use of the Meta Pixel on the Online Platforms, Defendant disclosed to Facebook:

a. Plaintiff's identity via his IP addresses and/or "c_user" cookies;

b. Plaintiff's seeking of medical treatment;

c. Plaintiff's status as a patient;

d. The pages and content Plaintiff viewed;

e. The providers Plaintiff viewed;

f. The treatment services Plaintiff viewed; and,

g. Information concerning Plaintiff's use of the patient portal, including to schedule appointments.

116. By failing to receive the requisite consent, Village breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

117. Plaintiff first discovered that Defendant was using the Meta Pixel and other tracking technologies to gather and disclose his Private Information in December of 2023.

118. As a result of Village's Disclosure of Plaintiff's Private Information via the Meta Pixel and other tracking technologies to third parties without authorization, Plaintiff now receives targeted health-related advertisements on Facebook for Village itself and for mental health outpatient clinics, reflecting his private medical treatment information.

119. Plaintiff paid Village for medical services and the services he paid for included reasonable privacy and data security protections for his Private Information, but Plaintiff did not receive the privacy and security protections for which he paid, due to Defendant's Disclosure.

120. Because of Defendant's unauthorized Disclosure of his Private Information, Plaintiff has suffered injuries, including monetary damages; loss of privacy; unauthorized disclosure of this Private Information; unauthorized access to his Private Information by third parties; use of the Private Information for advertising purposes; embarrassment, humiliation, frustration, and emotional distress; decreased value of his Private Information; lost benefit of the bargain; and increased risk of future harm resulting from further unauthorized use and disclosure of his information.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

121. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[87] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

122. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he

[87] Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective…at preventing the receipt of sensitive data."[88]

123. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[89] When a user was having his period or informed the app of his intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[90]

124. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[91]

---

[88] New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[89] Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[90] *Id.*
[91] Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document, VICE (April 26, 2022) https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

125. Furthermore, in June 2022, an investigation by The Markup[92] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[93] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[94] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[95]

126. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[96]

127. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta Pixel inside their password-protected patient portals.[97]

128. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply

[92] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* www.themarkup.org/about (last accessed Mar. 19, 2023).
[93] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*

troubled" by what the hospitals capturing and sharing patient data in this way.[98]

D. Defendant Violated HIPAA Standards

129. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[99]

130. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

131. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[100]

132. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or his protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis

---

[98] *Id.*
[99] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[100] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

added).[101]

133. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[102]

134. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[103]

135. Citing The Markup's June 2022 article, the Bulletin expressly notes:

> Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules**. For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.
>
> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more

[101] U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.
[102] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last acc. Apr. 3, 2024).
[103] *Id.*

> than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [104]

136. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel is a violation of HIPAA Rules.

E. Defendant Violated FTC Standards, and the FTC and HHS Take Action

137. The Federal Trade Commission ("FTC") has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[105]

138. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[106]

139. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules"[107] and that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing

---

[104] *Id.* (emphasis in original) (internal citations omitted).

[105] *Re: Use of Online Tracking Technologies*, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **Exhibit A.**

[106] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

[107] *Id.*

purposes."[108]

140. Entities that are not covered by HIPAA also face accountability for disclosing consumers' sensitive health information under the Health Breach Notification Rule. 16 C.F.R. § 318. This Rule requires that companies dealing with health records notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, *including sharing of covered information without an individual's authorization*, triggers notification obligations under the Rule."[109]

141. Additionally, the FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a). According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule."[110]

142. As such, the FTC and HHS have expressly stated that conduct like Defendant's runs afoul of the FTC Act and/or the FTC's Health Breach Notification Rule.

F. Defendant Violated Industry Standards

---

[108] *Id.*

[109] Statement of the Commission: On Breaches by Health Apps and Other Connected Devices, U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf) (emphasis added).

[110] *See, e.g., U.S. v. Easy Healthcare Corp.,* Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.,* FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc*; In the Matter of Flo Health Inc.,* FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

143. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

144. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Village and its physicians.

145. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

146. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

147. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

G. Plaintiff's and Class Members' Expectation of Privacy

148. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

H. IP Addresses are Personally Identifiable Information

149. On information and belief, Defendant also disclosed and otherwise assisted Facebook and potentially others with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other tracking technologies.

150. An IP address is a number that identifies the address of a device connected to the Internet.

151. IP addresses are used to identify and route communications on the Internet.

152. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

153. Facebook tracks every IP address ever associated with a Facebook user.

154. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

155. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

156. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

I. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

157. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

158. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

159. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

160. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

J. Plaintiff's and Class Members' Private Information Had Financial Value

161. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."[111] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[112] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested

[111] Audience Ad Targeting, Meta, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 14, 2023).
[112] *Id.*

in your business."[113]

162. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[114]

163. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

164. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both lucrative and a significant risk to privacy.[115]

165. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[116]

TOLLING, CONCEALMENT, AND ESTOPPEL

---

[113] *See* How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center, https://www.facebook.com/business/help/465262276878947 (last visited Aug. 14, 2023).
[114] *See* Here's How Big Facebook's Ad Business Really Is, CNN, https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html (last visited Aug. 14, 2023).
[115] *See* Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry, TIME, (Jan. 9, 2017 at 9:00 a.m.) https://time.com/4588104/medical-data-industry/.
[116] *See* Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

166. The applicable statutes of limitation have been tolled as a result of Village's knowing and active concealment and denial of the facts alleged herein.

167. Village seamlessly incorporated Meta Pixel and other trackers into its Website and Online Platforms while providing users with no indication that their Website usage was being tracked and transmitted to third parties. Village knew that its Website incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook and likely other third parties.

168. Plaintiff and Class Members could not with due diligence have discovered the full scope of Village's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel or any other tracking technology to unauthorizedly disclose their PHI/Private Information.

169. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Village's illegal interception and disclosure of Plaintiff's Private Information has continued unabated. What is more, Village was under a duty to disclose the nature and significance of its data collection practices but did not do so. Village is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

170. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all other similarly situated persons pursuant to Fed. R. Civ. P. 23.

171. The nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

172. Excluded from the Class are the following individuals and/or entities: Defendant

and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

173. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

174. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class is apparently identifiable within Defendant's records.

175. Commonality, Fed. R. Civ. P. 23(a)(2) and Predominance, Fed. R. Civ. P. 23(b)(3): : Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;

b. whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for unauthorized purposes;

e. whether Defendant failed to adequately Plaintiff's and Class Members' Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendant was negligent;

j. whether Defendant committed invasion of privacy—intrusion upon seclusion;

k. whether an implied contract existed between Plaintiff and the Class and Defendant;

l. whether Defendant breached its implied contracts with Plaintiff and the Class Members;

m. in the alternate, whether Defendant was unjustly enriched;

n. whether Defendant owed fiduciary duties to Plaintiff and the Class;

o. whether Defendant breached its fiduciary duties;

p. whether Defendant violated the Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.

q. whether Plaintiff and the Class Members are entitled to monetary damages, including compensatory and statutory damages, and the sums thereof.

176. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of Meta Pixel and other tracking technology.

177. Policies Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2): This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

178. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

179. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

180. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

181. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

182. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

183. Unless a Class-wide injunction is issued, Defendant may continue in their unlawful

disclosure and failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding Disclosure, and Defendant may continue to act unlawfully as set forth in this Complaint.

184. Further, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

185. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. whether Defendant committed an invasion of privacy—intrusion upon seclusion;

e. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied

contract;

f. whether Defendant breached the implied contract;

g. in the alternate, whether Defendant was unjustly enriched;

h. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;

i. whether Defendant failed to implement and maintain reasonable security procedures and practices;

j. whether Defendant owed fiduciary duties to Plaintiff and the Class;

k. whether Defendant breached its fiduciary duties;

l. whether Defendant violated the Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA"), 815 Ill. Comp. Stat. § 505/1, *et seq*.; and,

m. whether Plaintiff and the Class Members are entitled to actual, compensatory, consequential, and/or nominal damages, and punitive damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

186. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

187. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that

occurred.

188. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

189. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's Disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

190. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way of data harvesting, advertising, and increased sales.

191. Defendant breached its common law duties by failing to exercise reasonable care in the handling and securing of Private Information of Plaintiff and Class Members and in the supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private Information of Plaintiff and Class Members. This failure actually and proximately caused Plaintiff's and Class Members' injuries.

192. In addition, the standards of care owed by Defendant are established by statute, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections

identified above, under which Defendant were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Private Information.

193. Plaintiff and Class Members are within the class of persons that these statutes and rules were designed to protect.

194. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information, PII and PHI.

195. Defendant owed a duty to timely and adequately inform Plaintiff and Class Members, in the event of their Private Information, PII and PHI, being improperly disclosed to unauthorized third parties.

196. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information, PII and PHI, in compliance with applicable laws would result in an unauthorized third-parties such as Facebook, and others gaining access to Plaintiff's and Class Members' PII and PHI, and resulting in Defendant's liability under principles of negligence and negligence *per se*.

197. Defendant violated the standards of care under Section 5 of the FTC Act and under HIPAA and attendant regulations by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

198. As a direct and traceable result of Defendant's negligence and/or negligent supervision, and/or negligence *per se*, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements, and use of their Private

Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

199. Plaintiff's and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

200. Defendant's breach of its common-law duties to exercise reasonable care and negligence, and negligence *per se*, directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information and diminution in value, emotional distress, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent, immediate, and continuing.

201. In failing to secure Plaintiff's and Class Members' Private Information, PII and PHI, Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful, or conscious disregard of Plaintiff and Class Members' rights. Plaintiff, in addition to seeking actual damages, also seeks punitive damages on behalf of themselves and the Class.

202. Defendant's negligence directly and proximately caused the unauthorized access and Disclosure of Plaintiff's and Class Members' Private Information, PII and PHI, and as a result, Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's

negligence and negligence *per se*.

COUNT II
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

203. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

204. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website and Online Platforms and the communications platforms and services therein.

205. Plaintiff and Class Members communicated sensitive Private Information, PHI and PII, that they intended for only Defendant to receive and that they understood Defendant would keep private.

206. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion and their private affairs and concerns.

207. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations, Privacy Policies and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is highly offensive to the reasonable person.

208. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to invasion of their privacy rights, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred

to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's conduct. These injuries are ongoing, imminent, immediate, and continuing.

209. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

210. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to actual and compensatory damages, and all other relief they may be entitled to reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

211. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

212. Plaintiff also seek such other relief as the Court may deem just and proper.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

213. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

214. As a condition of receiving medical care from Defendant, Plaintiff and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiff and the Class entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in their Privacy Policies and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if Defendant "or one of [its] business associates, discover[s] an inappropriate use or disclosure of []

health information..."[117]

215. Implicit in the agreement between Village and its patients, Plaintiff and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

216. Village had an implied duty of good faith to ensure that the Private Information of Plaintiff and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Village.

217. Village had an implied duty to protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses.

218. Additionally, Village implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

219. Plaintiff and Class Members fully performed their obligations under the implied contract with Village. Village did not. Plaintiff and Class Members would not have provided their confidential Private Information to Village in the absence of their implied contracts with Village and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from Village.

220. Village breached the implied contracts with Plaintiff and Class members by disclosing Plaintiff's and Class Members' Private Information to an unauthorized third party.

221. Village's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their Private Information in exchange for medical treatment and benefits.

222. As a direct and proximate result of Defendant's above-described breach of

[117] *Notice of Privacy Practices,* Exhibit C.

contract, Plaintiff and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

223. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

224. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

225. This claim is pleaded solely in the alternative to Plaintiff's Breach of Implied Contract claim.

226. Plaintiff and Class members conferred a monetary benefit upon Village in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

227. Plaintiff and Class Members would not have used Village's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose their Private Information to third parties.

228. Village appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class members.

229. As a result of Village's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members

paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

230. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members themselves. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

231. Village should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Disclosure alleged herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

232. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

233. A relationship existed between Plaintiff and the Class, on the one hand, and Defendant, on the other, in which Plaintiff and the Class put their trust in Defendant to protect the Private Information of Plaintiff and the Class, and Defendant accepted that trust.

234. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, their Private Information.

235. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and damages to Plaintiff and the Class.

236. But for Defendant's breach of fiduciary duty, the injury-in-fact and damage to

Plaintiff and the Class would not have occurred.

237. Defendant's breach of fiduciary duty contributed substantially to producing the damage to the Plaintiff and the Class.

238. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VI
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE PRACTICES ACT ("CFDPA")
815 ILL. COMP. STAT. § 505/1, *ET SEQ.*
(On Behalf of Plaintiff and the Class)

239. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

240. The Illinois Consumer Fraud and Deceptive Practices Act ("CFDPA") makes it unlawful to employ "[u]nfair methods of competitions and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in [this section] . . . in the conduct of any trade or commerce." 815 Ill. Comp. Stat. § 505/2.

241. At all times relevant hereto, Defendant was engaged "in the conduct of trade or commerce" by hosting and publishing their Website that they encouraged their patients to use and where they advertised their healthcare services to the public. *Id.*

242. By conduct set forth in the preceding paragraphs, Village used unfair and deceptive acts or practices in the conduct of trade or commerce, including but not limited to the following:

a. Defendant encouraged its patients to use its Website and Online Platforms while representing its commitment to protecting the privacy of their Private Information, stating that, "[w]e will not use or disclose [patients'] health information, except as described in this document, unless [they] authorize us, in writing, to do so. […] Specific examples of uses or disclosures requiring written authorization include […] marketing activities, the sale of [] health information and most uses and disclosures for which [Village is] compensated[;]"[118] and that patients have "the right to be notified in the event that [Village], or one of [its] business associates, discover an inappropriate use or disclosure of your health information. Notification of any such use or disclosure will be made in accordance with state and federal requirements."[119]

b. Meanwhile, Defendant shared Plaintiff and Class Members' Private Information with Facebook and possibly others, without Plaintiff and Class Members' knowledge or consent.

c. Defendant promised that it would not use Plaintiff and Class Members' PHI for marketing purposes prior to obtaining their written permission. At the same time, Defendant knowingly collected Plaintiff's and Class Members' private information for marketing purposes. On information and belief, Defendant then used this information to market their services to Plaintiff and Class Members and thereby increase their profits.

[118] *Notice of Privacy Practices,* Exhibit C.
[119] *Id*.

d. Plaintiff and Class Members relied on Village's representations in using Village's Online Platform and thought they were communicating only with their trusted healthcare provider. In actuality, Defendant was surreptitiously intercepting and transmitting Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to Facebook.

243. Village's Disclosure of Plaintiff and Class Members' Private Information was willful, knowing, and done with intent that Plaintiff and Class Members rely upon the concealment, suppression or omission of a material fact: that Village was tracking Plaintiff's and Class Members' Private Information, using it for advertising purposes without their permission, and disclosing that information to unauthorized third parties.

244. The CFDPA provides that "[a]ny person who suffers actual damage as a result of a violation of this Act committed by any other person may bring an action against such person. The court, in its discretion may award actual economic damages or any other relief which the court deems proper." 815 Ill. Comp. Stat. Ann. 505/10a(a). Further, "the Court may grant injunctive relief where appropriate and may award, in addition to the relief provided in this Section, reasonable attorney's fees and costs to the prevailing party." *Id.* at 505/10a(b).

245. Had Plaintiff and members of the Class been aware that their Private Information would be transmitted to unauthorized third parties, they would not have entered into such transactions and would not have provided payment or confidential medical information to Village.

246. As a direct and proximate result of Defendant's unfair and deceptive acts and practices in violation of the CFDPA, Plaintiff and Class Members have suffered damages for which Defendant is liable, including, but not limited to, the following.

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private.

b. Defendant eroded the essential confidential nature of the doctor-patient relationship.

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value.

d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality.

e. Defendant's actions diminished the value of Plaintiff's and Class Members' personal information.

247. Plaintiff and Class Members seek actual damages plus interest on damages at the legal rate, as well as all other just and proper relief afforded by the CFDPA. As redress for Defendant's repeated and ongoing violations, Plaintiff and Class Members are entitled to, *inter alia*, actual damages, reasonable attorneys' fees and costs, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and Plaintiff's counsel as Class Counsel;

B. for an award of actual damages, compensatory damages, statutory damages, and

statutory penalties, in an amount to be determined, as allowable by law;

C. for an award of punitive damages, as allowable by law;

D. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

E. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

F. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

G. ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

H. for an award of reasonable attorneys' fees and costs under the CFDPA, the common fund doctrine, and any other applicable law;

I. costs and any other expenses, including expert witness fees incurred by Plaintiff in connection with this action;

J. pre- and post-judgment interest on any amounts awarded; and

K. such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, pursuant to 735 Illinois Compiled Statutes 5/2-1105, hereby demands a trial by jury on all issues so triable.

Dated: April 10, 2024

Respectfully submitted,

/s/Samuel J. Strauss

Samuel J. Strauss, Bar No. 6340331
Raina C. Borelli
TURKE & STRAUSS, LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Lynn A. Toops (*Pro Hac Vice* forthcoming)
Mary Kate Dugan (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Counsel for Plaintiff and the Proposed Class